

A simple block representation of reversible cellular automata with time-symmetry

Pablo Arrighi

*Université de Grenoble, LIG, 220 rue de la chimie, 38400 Saint-Martin-d'Hères, France
and École Normale Supérieure de Lyon, LIP, 46 Allée d'Italie, 69364 Lyon, France**

Vincent Nesme

QMIO, Freie Universität Berlin, Arnimallee 14, 14195 Berlin, Germany†

Reversible Cellular Automata (RCA) are a physics-like model of computation consisting of an array of identical cells, evolving in discrete time steps by iterating a global evolution G . Further, G is required to be shift-invariant (it acts the same everywhere), causal (information cannot be transmitted faster than some fixed number of cells per time step), and reversible (it has an inverse which verifies the same requirements). An important, though only recently studied special case is that of Time-symmetric Cellular Automata (TSCA), for which G and its inverse are related via a local operation. In this note we revisit the question of the Block representation of RCA, i.e. we provide a very simple proof of the existence of a reversible circuit description implementing G . This operational, bottom-up description of G turns out to be time-symmetric, suggesting interesting connections with TSCA. Indeed we prove, using a similar technique, that a wide class of them admit an Exact block representation (EBR), i.e. one which does not increase the state space.

Introduction

RCA, Block representation. In [Kar96], Kari showed that any one-dimensional or two-dimensional reversible cellular automaton (RCA) can be expressed as a composition of finite reversible gates (or ‘block permutations’) and partial shifts. In two dimensions the proof is quite involved, the representation requires three layers of blocks, and it has been proved that this cannot be brought down to a two-layered block representation [Kar99]; The problem is still open in higher dimensions.

However we may not need an exact representation, and be willing to encode our original cells into some larger ones (or equivalently to interleave some ancillary cells), as proposed in [DL01]. Then the construction of [Kar99] shows that even n -dimensional RCA admit a two-layered block representation. In some sense what we are doing then is simulating the original RCA in a way which preserves the spatial layout of cells, with another, simpler RCA that we know admits a two-layered block representation. In this sense the intrinsically universal RCA [DL95] also accomplishes this task.

Our Section I revisits this issue in a minimalistic manner: In our construction each block can be interpreted a reversible version of the local update rule of the CA, moreover its size turns out to be exactly that of the Block Neighborhood introduced in [AN10].

TSCA, EBRs. Recently another line of investigation has emerged which refines the now well-studied concept of RCA to admit a further requirement: That of time symmetry. In simple terms, a CA G is time-symmetric if G is its own inverse up to a simple recoding H of the cells. More formally, $G^{-1} = HGH$ with H a self-inverse CA. Credit must be given to [MG10] for emphasizing time-symmetry as a property of CA, which has barely been studied for its own sake thus far. It is clear nevertheless that many instances of time-symmetric CA (TSCA) can be encountered in the literature, as discussed in [MG10] (for instance the Margolus lattice gas model). In the above-discussed non-exact Block representation of RCA [Kar99] just like in ours, the author first encodes a RCA F into a TSCA G_F , and then provides an EBR of G_F . As a consequence, one may wonder whether these issues, block representations of RCA and TSCA are only accidentally related, or whether exhibiting a reversible local implementation mechanism for G amounts to unravelling the time-symmetry of G .

Our Section II begins to explore this issue by showing the existence of an EBR for squares of locally time-symmetric CA.

*Electronic address: Pablo.Arrighi@ens-lyon.fr

†Electronic address: Vincent.Nesme@qipc.org

I. A SIMPLE BLOCK REPRESENTATION

In the classical picture a CA G is usually defined by a local update rule δ , namely a function from $\Sigma^{\mathcal{N}}$ to Σ , giving the new state of a cell as a function of the old state of its neighbours; It can be thought as a ‘local mechanism’ for implementing G . In other words, δ can be viewed as a local gate, and G a circuit made by infinitely repeating δ across space as in Fig. 1.

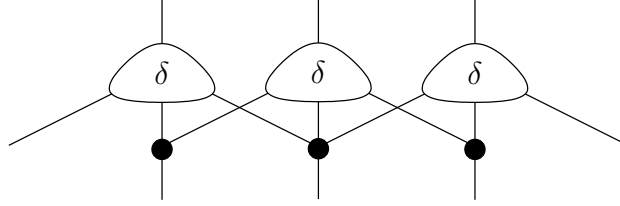


FIG. 1: The trivial circuit representation of a classical CA from its local update rule.

Using a local update rule to define RCA is of course possible, but for a circuit representation of G one may wish to use a local mechanism that is itself reversible — for instance in the context of quantum mechanical devices or due to Landauer’s principle. And indeed it is the case that every RCA G admits a reversible circuit implementation. Proving the existence of such reversible circuits is the business of the aforementioned block representation theorems for RCA. It could be regretted, however, that in these theorems the reversible local gates (a.k.a blocks) constitutive of the reversible circuits (a.k.a block representations) end up looking quite different from δ . I.e. they are hard to interpret as reversible versions of the local update rule.

The following proof of the block representation theorem for RCA is hopefully simpler to understand. It starts off by defining a reversible update operator K_0 , which can be interpreted as a reversible version of the local update rule δ . We will define K_0 globally, in a way that does not make it obvious that it is actually a block permutation — but we will then proceed to show that it is the case. Notice that it is impossible to implement CA of non-trivial Welch index — for a definition, cf. section 3 of [Kar96] — without shifts or auxiliary space: In our case, we use auxiliary space, which results in the collateral damage of implementing, in parallel to G , its inverse on the auxiliary strip.

Repeatedly we will define a bijection f from a set of words written on some fixed set of cells X , and then wonder whether f could be defined on a smaller subset. We will say that f is localized upon $Y \subseteq X$ if we can write $f = f_Y \times \text{id}_{Y \setminus X}$, i.e. if $Y \setminus X$ is superfluous in the definition of f . For instance, a bijection of $\Sigma^{\mathbb{Z}}$ that applies a permutation of the alphabet on cell 0 and leaves the other cells untouched is localized upon $Y \subseteq \mathbb{Z}$ if Y contains 0; The identity is localized on the empty set.

From the definition, it is obvious that if f is localized upon Y and $Y \subseteq Z \subseteq X$, then f is also localized upon Z . Slightly less trivial is the property that, whenever f is localized upon Y and Z , then it is also localized upon their intersection $Y \cap Z$. From there follows the existence of the smallest Y upon which f is localized, which is called the *localization* of f , and denoted $\text{Loc}(f)$. So, back to our elementary example where f is a permutation π of Σ applied solely on cell 0, $\text{Loc}(f) = \begin{cases} \emptyset & \text{if } \pi = \text{id} \\ \{0\} & \text{otherwise} \end{cases}$.

In general, K_0 is not localized upon the neighborhood of G . We will show however that its localization is \mathcal{BN} , the Block neighborhood defined in [AN10] whose definition we will recall. Hence it can thus be viewed as a block permutation of size $|\mathcal{BN}|$. The last step of the proof is just to show that G a circuit made by infinitely repeating K across space.

Reversible updates $K_i \dots$

In the classical picture, the local update rule δ looks at a neighborhood $\dots c_{-1}c_0c_1 \dots$ and computes $G(c)_0$, but it leaves all the other cells uncomputed. Can we, in a similar fashion, define a reversible update K_0 which focuses on computing $G(c)_0$? Moreover can we, in an again a similar fashion, define it solely in terms of G ? A naive, operational approach would be to: 1. Apply G . 2. Swap $G(c)_0$ out of the system. 3. Apply G^{-1} . This will turn out to work. Technically, we will extend the alphabet to Σ^2 . For i running over all cells, we denote by S_i the swap acting only on position i according to $\begin{pmatrix} \Sigma^2 & \rightarrow & \Sigma^2 \\ (a, b) & \mapsto & (b, a) \end{pmatrix}$.

Definition 1 (reversible update) *The reversible update K_i is the function from $\mathcal{C}_{\Sigma^2} \simeq \mathcal{C}_{\Sigma}^2$ to itself given by the following composition*

$$K_i = (G^{-1} \times \text{id}) S_i (G \times \text{id})$$

where \mathcal{C}_{Σ} denotes the space of configurations of cells having alphabet Σ .

We can right now formulate the important remark that the K_i -s commute. We will later prove with Proposition 1 that each K_i , despite being defined globally, is actually a local permutation, acting in some neighborhood of cell i ; Let us admit this fact within this paragraph. With these informations in mind, it makes sense to define the infinite product $\prod_i K_i$. Indeed, for any given cell, the number of K_i -s acting on this cell is finite; Therefore the composition of all the K_i -s can be written as a circuit of finite depth and is thus perfectly well-defined. Moreover, it is equal to $(G^{-1} \times \text{id}) S (G \times \text{id})$, where $S = \prod_i S_i$. Therefore we have $S \prod_i K_i = G \times G^{-1}$.

Let us take a closer at K_0 . Start with a configuration $\dots (c_i, d_i) \dots$. Applying $G \times \text{id}$ takes it to $\dots (G(c)_i, d_i) \dots$. Then S_0 turns it into

$$\dots (G(c)_{-2}, d_{-2}), (G(c)_{-1}, d_{-1}), (d_0, G(c)_0), (G(c)_1, d_1), (G(c)_2, d_2) \dots$$

So K_0 leaves the second component unchanged, except in position 0. In fact, the rest of the second component could be left out in the definition of K_0 , since it plays no role. Specifically, one can write K_0 as a product of the identity on these cells and of some bijection of $\mathcal{C}_{\Sigma} \times \Sigma$. The left component, after applying K_0 , finds itself in the state $G^{-1}(\dots G(c)_{-2} G(c)_{-1} d_0 G(c)_1 G(c)_2 \dots)$. Of course, outside of some neighborhood of 0, this is the identity; But that triviality alone is not enough to conclude that K_0 is localized upon a finite number of cells. We are going to check that it is indeed the case, and moreover that its localization is a rather remarkable set.

... are localized within the Block Neighborhood \mathcal{BN} ...

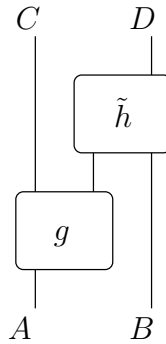


FIG. 2: Semilocalizability.

In [AN10], the authors introduced the block neighborhood \mathcal{BN} of a RCA, using the concept of semilocalizability that appeared in [ESW02] in the context of quantum information theory. Given a bijection $F : X \rightarrow Y$ and a decomposition of X and Y in respectively $A \times B$ and $C \times D$, F is said to be semilocalizable (with respect to this decomposition) when it can be written in the form of Figure 2, where g and \tilde{h} are themselves bijections. The quantum neighborhood of a RCA F is then the smallest subset \mathcal{BN} such that, as a function from $\Sigma^{\mathcal{BN}} \times \Sigma^{\mathcal{BN}}$ to $\Sigma^{\{0\}} \times \Sigma^{\{0\}}$, F is semilocalizable — see Figure 3 for an illustration.

The definition of the block neighborhood was motivated by the fact that it is both the (quantum) neighborhood of the quantum CA obtained by linearization from a RCA, and obviously related to the decomposition of a QCA into a product of local permutations, a link that we make more precise in this article. More details on \mathcal{BN} are to be found in [AN10], where it is the object of definition 1.9, and where explicit bounds on \mathcal{BN} are given in function of the neighborhoods of G and of its inverse. We will not need these bounds, except for the fact that they do prove that \mathcal{BN} is finite:

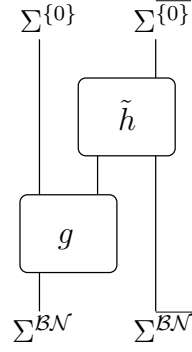


FIG. 3: The block neighborhood.

- \mathcal{BN} is included in $(\mathcal{N} - \mathcal{N} + \tilde{\mathcal{N}}) \cap (\tilde{\mathcal{N}} - \tilde{\mathcal{N}} + \mathcal{N})$, with $\tilde{\mathcal{N}}$ the transpose of the inverse neighborhood \mathcal{N}^{-1} . There are examples saturating this bound;
- $\mathcal{BN}(G^k)/k$ tends towards $\mathcal{N}(G^k) \cup \tilde{\mathcal{N}}(G^k)$ in the limit where k goes to infinity, with $\mathcal{BN}(G^k)$ the Block Neighborhood of G^k etc.

In the definition of K_0 , cells are divided into two subcells, so that these subcells are naturally indexed by $\{0, 1\} \times \mathbb{Z}$. We now prove that the localization of K_0 is essentially the block neighborhood \mathcal{BN} ; As \mathcal{BN} is also the *quantum* neighborhood, i.e. the neighborhood when inputs are not just words but can be linear combination on words (cf. [AN10]), this gives a nice way to characterize the quantum dynamics in a purely classical setting.

Proposition 1 *Consider a RCA G , and let K_0 be its reversible update. Then $\text{Loc}(K_0) = \{0\} \times \mathcal{BN} \cup \{(1, 0)\}$.*

Proof. $[\subseteq]$. Consider a $\tilde{h}g$ -decomposition of G in the manner of Figure 3. Then g is localized upon \mathcal{BN} , \tilde{h} outside of cell 0, and

$$\begin{aligned}
 K_0 &= (G^{-1} \times \text{id})S_0(G \times \text{id}) \\
 &= ((\tilde{h}g)^{-1} \times \text{id})S_0((\tilde{h}g) \times \text{id}) \\
 &= (g^{-1} \times \text{id})(\tilde{h}^{-1} \times \text{id})S_0(\tilde{h} \times \text{id})(g \times \text{id}) \\
 K_0 &= (g^{-1} \times \text{id})S_0(g \times \text{id})
 \end{aligned}$$

where the last line follows from the fact that $\text{Loc}(\tilde{h})$ does not contain $\{0\}$, whereas S_0 is localized upon cell 0. From this last line we can read $\text{Loc}(K_0) \subseteq \{0\} \times \mathcal{BN} \cup \{(1, 0)\}$.

$[\supseteq]$. *Note that this second inclusion is no needed for the proof of the Block representation; It is provided here just for completeness.* As we have already mentioned, $\text{Loc}(K_0)$ is of the form $\text{Loc}(K_0)_0 \cup \{(1, 0)\}$. So $\text{Loc} \prod_{n \neq 0} K_n$ does

not contain $(1, 0)$. But $K_0 \prod_{n \neq 0} K_n = (G^{-1} \times \text{id})S(G \times \text{id})$. For $a \in \Sigma$, let X_a be the subset of words on $\text{Loc}(K_0)$

that are equal to a on $(1, 0)$. The image of X_a by $S_0(G \times \text{id})$ is of the form $Y_a \times \Sigma$, where Y_a is the set of words on $\text{Loc}(K_0)_0 \cup \{(0, 0)\}$ that are equal to a in $(0, 0)$, and Σ is localized on $(1, 0)$. Therefore the image of X_a by K_0 is also of the form $Z_a \times \Sigma$ for some subset Z_a of the words on $\text{Loc}(K_0)_0$.

Furthermore, we know that there exists a bijection finishing the job after the isolation of $G(c)_0$ by K_0 , namely $\prod_{n \neq 0} K_n$. We must thus have a semilocalization of G with respect to $\text{Loc}(K_0)_0$: In figure 3, K_0 plays the role of g ,

\mathcal{BN} is $\text{Loc}(K_0)_0$, and \tilde{h} is $\prod_{n \neq 0} K_n$. Since \mathcal{BN} is the smallest set fulfilling this property, it must then be included in $\text{Loc}(K_0)_0$. ■

...and thus implement G .

Combining the above results we obtain the following:

Corollary 1 ($G \times G^{-1} = S(\prod K)$) Consider a RCA G , and let K be its reversible update. Consider the function $G \times G^{-1}$ from \mathcal{C}_Σ^2 to \mathcal{C}_Σ^2 . We have that

$$G \times G^{-1} = S \prod_i K_i \quad \text{with} \quad \text{Loc}(K_0) = \{0\} \times \mathcal{BN} \cup \{(1, 0)\}.$$

Hence we have here a proof that all RCA admit a block representation, the third of its genre [Kar96, DL01], but hopefully also the most straightforward, as it simply takes the form a product of reversible updates. There is one bad and one good news about this proof. The bad news is that it provides only a non-exact Block representation of RCA, leaving it open whether $n > 2$ -dimensional RCA admit an EBR or not. The good news is that it provides an EBR for those TSCA which are of the form $G \times G^{-1}$. This suggests that we should look at the relation between EBRs and time-symmetry of CA.

II. EBRs AND TIME-SYMMETRY

The core of the argument that we developed in the previous section for the existence of an EBR for $G \times G^{-1}$ could be restated as follows: Say F and H are RCA such that H admits an EBR, then so does FHF^{-1} ! Indeed, if $H = \prod_i B_i$, then $FHF^{-1} = \prod_i FB_iF^{-1}$. Moreover following Proposition 1. [⊆], the blocks FB_iF^{-1} are localized, at most, on the localization of B_i extended by $\mathcal{BN}(F)$ the block neighborhood of F ; Hence each of them is finitely localized, i.e. is itself a block permutation.

In Section I we applied this argument with $F = G^{-1} \times \text{id}$ and $H = S$, which admits a trivial block representation $S = \prod_{n \in \mathbb{Z}} S_n$. This gave an EBR of $(G^{-1} \times \text{id})S(G \times \text{id})$, which is only a swap away from $G \times G^{-1}$. In fewer words, $G \times G^{-1}$ admits an EBR because the set of RCA having this property

- contains the permutations of Σ , and
- is a normal subgroup of the group of RCA.

Having generalized this procedure, let us now have a look at what it tells us in the context of TSCA.

Definition 2 (Locally Time-Symmetric CA) A RCA G is a locally time-symmetric CA (LTSCA) if there exists an involution h of Σ such that $G^{-1} = HGH$, with $H = \prod_i h_i$.

Our definition of LTSCA is identical to that of TSCA given in [MG10] except for one extra condition: We further demand that the RCA H be of radius zero. On this question of the locality of H , let us quote the authors of this first paper introducing TSCA [MG10]: “Requiring H to be a CA is somewhat arbitrary, [...] the reason for this restriction is that we expect reversibility (including the particular case of time-symmetry) to be a local property.”. Moreover, whilst the theoretical results they prove are valid for H an involution RCA of arbitrary radius, it is also true that in all of the examples provided, H is of radius zero. In fact, one may wonder whether there LTSCA and TSCA are not equivalent up to a simple encoding.

Anyhow, if H has radius zero, then in particular it admits an EBR, and so does $GHG^{-1}H = G^2$. Therefore, the squares of LTSCA have EBRs:

Corollary 2 (EBR of LTSCA²) Let G be an LTSCA with respect to an involution h . We have $G^2 = H \prod_i L_i$, where $L_i = G^{-1}h_iG$, furthermore $\text{Loc}(B_0) \subseteq \mathcal{BN}$.

Some remarks are in order:

- h_0 plays the role that S_0 had in section I. Likewise, in the standard examples of TSCA [MG10], H can be interpreted as a swap. This is certainly the case in particular for the standard time-symmetrizations $G \times G^{-1}$ of any RCA G , as in Prop. 5.3. of [MG10].
- This time the block representation is an exact one, hence it is remarkable that LTSCA have this property given the difficulty of finding the EBRs of $n > 2$ -dimensional RCA. Nevertheless, the representation applies to G^2 and not G itself. Simply proving that any involutive RCA admits an EBR is probably difficult, as it gets dangerously close to solving the aforementioned open problem.

Conclusion

Generalizations. As in [AN10], the block representation defined in Section I, and the proof that it is of minimal size, rely only on notions on neighborhood, while others characteristics of CA, such as finiteness of the alphabet and translation invariance, are simply irrelevant. Moreover, whilst the arguments we have provided in this paper are purely classical, they have their counterparts in the field of quantum CA [SW04], some of which were of direct inspirations to this paper [ANW11]. Part of our motivation was to make these techniques available to classical CS.

Questions, answers and more questions. Why is time-symmetry such a key step Block representations of RCA? In this paper gave a simple proof of the block representation of RCA, which partly explains this role. Could it be that TSCA admit an EBR? In this paper we gave a simple proof of the EBR of squares of LTSCA. These are all but partial answers, suggesting that many questions remain on the topic of understanding differences in structure between RCA and TSCA, TSCA and LTSCA. There might lie a path towards EBRs of RCA in arbitrary dimensions.

Acknowledgments

The authors would like to thank Jarkko Kari, Anahí Gajardo, and funding by the Deutsche Forschungsgemeinschaft (Forschergruppe 635) and ANR JJC CCausaQ.

-
- [AN10] Pablo Arrighi and Vincent Nesme. The Block Neighborhood. In TUCS, editor, *Proceedings of JAC 2010*, pages 43–53, Turku, Finlande, December 2010.
 - [ANW11] Pablo Arrighi, Vincent Nesme, and Reinhard F. Werner. Unitarity plus causality implies localizability. *Journal of Computer and System Sciences*, 77(2):372–378, March 2011.
 - [DL95] Jérôme Durand-Lose. Reversible cellular automaton able to simulate any other reversible one using partitioning automata. In *Proceedings of the Second Latin American Symposium on Theoretical Informatics*, LATIN '95, pages 230–244, London, UK, 1995. Springer-Verlag.
 - [DL01] Jérôme Durand-Lose. Representing reversible cellular automata with reversible block cellular automata. In Robert Cori, Jacques Mazoyer, Michel Morvan, and Rémy Mosseri, editors, *Discrete Models: Combinatorics, Computation, and Geometry, DM-CCG '01*, volume AA of *Discrete Mathematics and Theoretical Computer Science Proceedings*, pages 145–154, 2001.
 - [ESW02] T. Eggeling, Dirk Schlingemann, and Reinhard F. Werner. Semilocal operations are semilocalizable. *Europhysics Letters*, 57(6):782–788, 2002.
 - [Kar96] Jarkko Kari. Representation of reversible cellular automata with block permutations. *Mathematical Systems Theory*, 29(1):47–61, 1996.
 - [Kar99] Jarkko Kari. On the circuit depth of structurally reversible cellular automata. *Fundam. Inf.*, 38(1-2):93–107, 1999.
 - [MG10] Andrés Moreira and Anahí Gajardo. Time-symmetric Cellular Automata. In TUCS, editor, *Proceedings of JAC 2010*, pages 180–190, Turku, Finlande, December 2010.
 - [SW04] Benjamin Schumacher and Reinhard F. Werner. Reversible quantum cellular automata. [arXiv:quant-ph/0405174](https://arxiv.org/abs/quant-ph/0405174), May 2004.